

Notice of Allowability

Application No.

09/888,176

Examiner

Thomas M Ho

Applicant(s)

CHALLENGER ET AL.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 6/22/01.
2. ☒ The allowed claim(s) is/are 1-12.
3. ☒ The drawings filed on 06 August 2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. Claims 1 –12 are pending.
2. Claims 1-12 are allowable.

Reasons for Allowance

3. Claim 1 recites:

A method for migrating a base chip key from a first computer system to a second computer system, wherein said first computer system includes a base chip key 1, and said second computer system includes a base chip key 2, said method comprising:

Generating a second certificate for said base chip key 1 by a manufacturer of said second computer system using a first certificate for said base chip key 1, and generating a second certificate for said base chip key 2 by a manufacturer of said first computer system using a first certificate for said base chip key 2.

Sending a first data packet from said first computer system to said second computer system, wherein said first data packet includes all data necessary to reproduce said base chip key 1 in said second computer system.

Art Unit: 2134

Sending a second data packet from said second computer system to said first computer system acknowledging the receipt of a copy of said base chip key 1;

Erasing said base chip key 1 from said first computer system

Replacing said base chip key 2 in said second computer system with said base chip key 1.

Claim 7 is a computer program product substantially similar to the elements of claim 1.

US patent 5745576 Abraham et al. discloses a method and apparatus for the initialization of a cryptographic terminal.

Abraham et al. discloses:

Two computer systems, the first computer system with a first base key, and a second computer system with a second base key, where the first computer is sold to the Acme Company, and the second is sold to the Baker company. (Column 6, lines 57-66), where it is the manufacturer that generates the base keys.

Nordenstam et al. (Figure 2) discloses:

- a first certificate for a first base key and a second certificate for a second base key, where the first certificate is the CERT 1 in the distributing unit, the first base key is private key 1, the second base key is private key 2(in item 20), and the first certificate for the second base key is CERT 2.
- Sending a first data packet from said first computer system to said second computer system, wherein said first data packet includes all data necessary to reproduce said base chip key 1 in said second computer system, where the first data packet is the encrypted key information K and is sent from the distributing unit to the receiving unit (Column 8, lines 17-21), and where the data from the packet is regenerated into the base chip key 1, the private key. (Column 8, lines 37-41)
- Replacing said base chip key 2 in said second computer system with said base chip key 2, is replaced by the key that was sent by the distributing unit. (Column 4, lines 50-51)

The SSL 3.0 Specification(Section 7.5 6th paragraph, and Section 7.6.9) discloses:

- Sending a second data packet from said second computer system to said first computer system acknowledging the receipt of a copy of said base chip key 1, where base chip key 1, is the key that was transferred, and the second data packet is a finished message sent by the client to the server telling that the key transfer was successful.

Neither Abraham et al, Nordenstam et al., nor SSL 3.0 Specification disclose

- Erasing said base chip key 1 from said first computer system, where the base chip key 1 is the private key and can be erased.

Nordenstam et al., however, does disclose

- Erasing said base chip key 1 from a computer system, where the base chip key 1 is the private key and can be erased. (Column 4, lines 35-45)

Neither Abraham et al, Nordenstam et al., nor SSL 3.0 Specification disclose:

- Generating a second certificate for said base chip key 1 by a manufacturer of said second computer system using a first certificate for said base chip key 1, and generating a second certificate for said base chip key 2 by a manufacturer of said first computer system using a first certificate for said base chip key 2.

The Examiner notes that, while it would be unusual to generate a second certificate for a key, the generation process would merely involve the creation of a certificate a second time and would be obvious to those of ordinary skill in the art.

No reference, or combination of references can be found though, which would generate a second certificate from a first certificate for two disparate base chip keys by the manufacturer of each of the systems.

Conclusion

4. The following art not relied upon is made of record:
- US patent 6,160,890 discloses a secret key transfer method using multiple keys.
 - US patent 6,192,130 discloses a method of transferring a key history.
 - US patent 6,038,322 and 6,215,878 discloses a method of key distribution through the use of certificates and certificate authorities.


5. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER

Application/Control Number: 09/888,176
Art Unit: 2134

Page 7

TMH

January 21st, 2005